AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended.) A method for establishing secure communication between a calling party and a called party, consisting essentially of:

identifying a first shared random number associated with a ~~calling~~ called party;

identifying a second shared random number associated with a ~~called~~ calling party;

~~identifying said calling party to said called party;~~

said called party generating a public-private key pair ~~by said called party~~ including a public key and a private key;

transmitting a first message from said called party to said calling party, said first message including said first shared random number and said public ~~portion~~ key of said public-private key pair, ~~and~~ said first message being encoded with a symmetric encryption key;

transmitting a second message from said calling party to said called party, said second message including said second shared random number, ~~and~~ said second message being encoded with said public ~~portion~~ key of said public-private key pair; and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

2. (Previously Presented.) The method of claim 1, wherein said combining function includes a logical function.

3. (Previously Presented.) The method of claim 2, wherein said logical function includes an exclusive or (XOR) function.

4. (Cancelled.)

5. (Cancelled.)

6. (Currently Amended.) The method of claim ~~5~~1, wherein said first message is encoded using an encoded password.

7. (Previously Presented.) The method of claim 6, wherein said encoded password is an encrypted password.

8. (Currently Amended.) The method of claim 6, ~~wherein said step of encoding said first message comprises~~further comprising encrypting said first message using said encoded password.

9. (Cancelled.)

10.–153. (Cancelled.)

154 (New). A method for establishing secure communication between a calling party and a called party, comprising:

generating, on demand at the called party, an asymmetric key pair including a public key and a private key;

transmitting, from said called party to said calling party, a first encrypted message including a first random number and said public key of said asymmetric key

pair, said called party encrypting said first message with a symmetric encryption key known to the calling party;

said calling party receiving and decrypting said first encrypted message using said symmetric encryption key to obtain said first random number and said public key;

said calling party transmitting, to said called party, a second encrypted message including a second random number, said calling party encrypting said second message with said public key of said asymmetric key pair;

said called party receiving and decrypting said second encrypted message to obtain said second random number;

said calling and called parties each independently applying said now-shared first and second random numbers to combining functions to thereby each independently generate a shared secret key; and

said calling and called parties encrypting further communications therebetween at least in part using said shared secret key.

155 (New). The method of claim 154 wherein said symmetric encryption key comprises a password.